НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-05-27.1 | 27 мая 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-24851	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
2	Высокая	CVE-2024-24946	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
3	Высокая	CVE-2024-24947	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
4	Высокая	CVE-2024-24954	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
5	Высокая	CVE-2024-24955	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
6	Высокая	CVE-2024-24956	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
7	Высокая	CVE-2024-24957	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
8	Высокая	CVE-2024-24959	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
9	Высокая	CVE-2024-24962	AutomationDirect Productivity PLCs	Сетевой	ACE	2024-05-24	✓
10	Высокая	CVE-2024-24963	AutomationDirect Productivity PLCs	Сетевой	ACE	2024-05-24	✓
11	Критическая	CVE-2024-22187	AutomationDirect Productivity PLCs	Сетевой	SB	2024-05-24	✓
12	Критическая	CVE-2024-23315	AutomationDirect Productivity PLCs	Сетевой	OSI	2024-05-24	✓
13	Критическая	CVE-2024-21785	AutomationDirect Productivity PLCs	Сетевой	OSI	2024-05-24	✓

14	Критическая	CVE-2024-23601	AutomationDirect Productivity PLCs	Сетевой	ACE	2024-05-24	✓
15	Высокая	CVE-2024-24958	AutomationDirect Productivity PLCs	Сетевой	DoS	2024-05-24	✓
16	Высокая	CVE-2024-20360	Cisco Firepower Management Center	Сетевой	ACE	2024-05-27	✓
17	Высокая	CVE-2024-4978	Justice AV Solutions Viewer software	Сетевой	OSI	2024-05-24	✓
18	Высокая	CVE-2024-5274	Microsoft Edge	Сетевой	ACE	2024-05-26	✓
19	Высокая	CVE-2024-5158	Microsoft Edge	Сетевой	ACE	2024-05-26	✓
20	Высокая	CVE-2024-5157	Microsoft Edge	Сетевой	ACE	2024-05-26	✓
21	Высокая	CVE-2024-5160	Microsoft Edge	Сетевой	ACE	2024-05-26	✓
22	Высокая	CVE-2024-5159	Microsoft Edge	Сетевой	ACE	2024-05-26	✓
23	Критическая	CVE-2024-1597	Не определено	Сетевой	ACE	2024-05-24	✓
24	Высокая	CVE-2024-4947	Google ChromeOS TLS	Сетевой	ACE	2024-05-24	✓
25	Высокая	CVE-2024-5274	Google Chrome	Сетевой	ACE	2024-05-24	✓
26	Высокая	CVE-2024-4761	Google ChromeOS TLS	Сетевой	ACE	2024-05-24	✓
27	Высокая	CVE-2024-5274	Google Chrome	Сетевой	ACE	2024-05-24	✓
28	Высокая	CVE-2024-5040	LCDS LAquis SCADA	Локальный	RLF	2024-05-23	✓

29	Критическая	CVE-2024-29822	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
30	Критическая	CVE-2024-29823	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
31	Критическая	CVE-2024-29824	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
32	Критическая	CVE-2024-29825	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
33	Критическая	CVE-2024-29826	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
34	Критическая	CVE-2024-29827	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
35	Высокая	CVE-2024-29828	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
36	Высокая	CVE-2024-29829	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
37	Высокая	CVE-2024-29830	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
38	Высокая	CVE-2024-29846	Ivanti Endpoint Manager	Смежная сеть	ACE	2024-05-22	✓
39	Критическая	CVE-2023-51637	Sante PACS Server PG	Сетевой	ACE	2024-05-22	✓
40	Высокая	CVE-2024-5160	Google Chrome	Сетевой	ACE	2024-05-22	✓
41	Высокая	CVE-2024-5159	Google Chrome	Сетевой	ACE	2024-05-22	✓

42	Высокая	CVE-2024-5158	Google Chrome	Сетевой	ACE	2024-05-22	✓
43	Высокая	CVE-2024-5157	Google Chrome	Сетевой	ACE	2024-05-22	✓
44	Высокая	CVE-2024-33599	GNU Glibc	Сетевой	ACE	2024-05-21	✗
45	Высокая	CVE-2024-23980	Intel Server Products UEFI Firmware	Локальный	ACE	2024-05-22	✓
46	Высокая	CVE-2024-24981	Intel Server Products UEFI Firmware	Локальный	PE	2024-05-22	✓
47	Высокая	CVE-2024-4835	GitLab Community Edition и Enterprise Edition (EE)	Сетевой	XSS\CSS	2024-05-23	✓
48	Высокая	CVE-2024-23487	Intel Server Products UEFI Firmware	Локальный	PE	2024-05-22	✓
49	Высокая	CVE-2024-22382	Intel Server Products UEFI Firmware	Локальный	PE	2024-05-22	✓
50	Высокая	CVE-2024-0801	Arcserve Unified Data Protection	Сетевой	DoS	2024-05-16	✓
51	Высокая	CVE-2024-0800	Arcserve Unified Data Protection	Сетевой	WLF	2024-05-16	✓
52	Высокая	CVE-2024-32636	Siemens Parasolid	Локальный	OSI	2024-05-17	✓
53	Высокая	CVE-2024-31980	Siemens Parasolid	Локальный	ACE	2024-05-17	✓
54	Высокая	CVE-2024-32635	Siemens Parasolid	Локальный	OSI	2024-05-17	✓
55	Критическая	CVE-2024-0799	Arcserve Unified Data Protection	Сетевой	SB	2024-05-16	✓

1

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24851

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

2

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24946

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

3

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24947

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

4

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24954

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

5

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24955

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

6

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24956

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

7

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24957

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

8

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24959

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

9

Краткое описание: Выполнение произвольного кода в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24962

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

Краткое описание: Выполнение произвольного кода в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24963

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

10

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

11

Краткое описание: Обход безопасности в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-22187

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

12

Краткое описание: Получение конфиденциальной информации в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-23315

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

13

Краткое описание: Получение конфиденциальной информации в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-21785

Идентификатор программной ошибки: CWE-489 Присутствует код отладки

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

14

Краткое описание: Выполнение произвольного кода в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-23601

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

Краткое описание: Отказ в обслуживании в AutomationDirect Productivity PLCs

Идентификатор уязвимости: CVE-2024-24958

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Productivity 3000 P3-550E CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-550 CPU: 1.2.10.9 - 4.1.1.10
Productivity 3000 P3-530 CPU: 1.2.10.9 - 4.1.1.10
Productivity 2000 P2-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-550 CPU: 1.2.10.10 - 4.1.1.10
Productivity 1000 P1-540 CPU: 1.2.10.10 - 4.1.1.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01

16

Краткое описание: Выполнение произвольного кода в Cisco Firepower Management Center

Идентификатор уязвимости: CVE-2024-20360

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Cisco Firepower Management Center: 7.0.0 - 7.3.1.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-27 / 2024-05-27

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs

17

Краткое описание: Получение конфиденциальной информации в Justice AV Solutions Viewer software

Идентификатор уязвимости: CVE-2024-4978

Идентификатор программной ошибки: CWE-506 Внедренный вредоносный код

Уязвимый продукт: JAVS Viewer: 8.3.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://twitter.com/2RunJack2/status/1775052981966377148
- http://github.com/advisories/GHSA-wf54-f8v9-v72v
- http://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5274

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.51

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

18 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-26 / 2024-05-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5274

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5158

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.51

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

19 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-26 / 2024-05-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5158

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5157

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.51

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

20 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-26 / 2024-05-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5157

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5160

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.51

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-26 / 2024-05-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5160

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-5159

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 125.0.2535.51

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-26 / 2024-05-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-5159

Краткое описание: Выполнение произвольного кода в

Идентификатор уязвимости: CVE-2024-1597

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Jira Software: 9.0.0 - 9.15.1
Jira Data Center: 9.0.0 - 9.15.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

23

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://jira.atlassian.com/browse/JSWSERVER-25896
- https://bdu.fstec.ru/vul/2024-01541

24

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-4947

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Chrome OS: до 120.0.6099.312

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/long-term-support-channel-update-for_23.html
- https://bdu.fstec.ru/vul/2024-03978

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5274

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.77

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

25 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
- http://crbug.com/341663589

Краткое описание: Выполнение произвольного кода в Google ChromeOS TLS

Идентификатор уязвимости: CVE-2024-4761

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 120.0.6099.312

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

26 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/long-term-support-channel-update-for_23.html

27

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5274

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.77

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-24 / 2024-05-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
- http://crbug.com/341663589

Краткое описание: Чтение локальных файлов в LCDS LAquis SCADA

Идентификатор уязвимости: CVE-2024-5040

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: LAquis SCADA: 4.7.1.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

28

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-23 / 2024-05-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-142-01
- http://www.zerodayinitiative.com/advisories/ZDI-24-485/
- http://www.zerodayinitiative.com/advisories/ZDI-24-486/
- http://www.zerodayinitiative.com/advisories/ZDI-24-487/
- http://www.zerodayinitiative.com/advisories/ZDI-24-488/
- http://www.zerodayinitiative.com/advisories/ZDI-24-489/
- http://www.zerodayinitiative.com/advisories/ZDI-24-490/
- http://www.zerodayinitiative.com/advisories/ZDI-24-484/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29822

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

29 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29823

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

30 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29824

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

31 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29825

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

32 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29826

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

33 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29827

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

34 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.6 AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29828

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

35 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29829

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

36 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29830

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

37 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29846

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: с версии 2022 по 2022 SU5

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

38

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US
- http://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024?language=en_US

Краткое описание: Выполнение произвольного кода в Sante PACS Server PG

Идентификатор уязвимости: CVE-2023-51637

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: PACS Server PG: до версии 3.3.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

39

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-468/

40

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5160

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 125.0.6422.61

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
- http://crbug.com/338161969

41

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5159

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 125.0.6422.61

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
- http://crbug.com/335613092

42

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5158

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 125.0.6422.61

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
- http://crbug.com/338908243

43

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5157

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 125.0.6422.61

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
- http://crbug.com/336012573

Краткое описание: Выполнение произвольного кода в GNU Glibc

Идентификатор уязвимости: CVE-2024-33599

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Glibc: с версии 2.15 по 2.39.9000

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

44 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-21 / 2024-05-21

Ссылки на источник:

- http://sourceware.org/git/?p=glibc.git;a=blob;f=advisories/GLIBC-SA-2024-0005
- https://bdu.fstec.ru/vul/2024-03561

Краткое описание: Выполнение произвольного кода в Intel Server Products UEFI Firmware

Идентификатор уязвимости: CVE-2024-23980

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Intel Server D50FCP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера

Последствия эксплуатации: Выполнение произвольного кода

45 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html

Краткое описание: Повышение привилегий в Intel Server Products UEFI Firmware

Идентификатор уязвимости: CVE-2024-24981

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Intel Server M50FCP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

46 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html

Краткое описание: Межсайтовый скриптинг в GitLab Community Edition и Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2024-4835

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: GitLab Enterprise Edition и Community Edition:
Gitlab Community Edition: с версии 15.11.0 по 17.0.0
GitLab Enterprise Edition: с версии 15.11.0 по 17.0.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

47 **Последствия эксплуатации:** Межсайтовый скриптинг

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.0 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-23 / 2024-05-23

Ссылки на источник:

- http://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/

Краткое описание: Повышение привилегий в Intel Server Products UEFI Firmware

Идентификатор уязвимости: CVE-2024-23487

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Intel Server D50DNP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

48 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html

Краткое описание: Повышение привилегий в Intel Server Products UEFI Firmware

Идентификатор уязвимости: CVE-2024-22382

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Intel Server D50DNP: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

49 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-22 / 2024-05-22

Ссылки на источник:

- http://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html

Краткое описание: Отказ в обслуживании в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0801

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Unified Data Protection: до версии 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

50 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07

Краткое описание: Запись локальных файлов в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0800

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Unified Data Protection: до версии 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Запись локальных файлов

51 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-32636

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: с версии 35.1 по 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

52 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-046364.html

53

Краткое описание: Выполнение произвольного кода в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-31980

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Parasolid: с версии 35.1 по 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-489698.html
- https://bdu.fstec.ru/vul/2024-03945

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-32635

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: с версии 35.1 по 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

54 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-046364.html

55

Краткое описание: Обход безопасности в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0799

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Unified Data Protection: до версии 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07
- https://bdu.fstec.ru/vul/2024-02247